European Patent Application
"Message Authentication"
Sony International (Europe) GmbH
S99P5143EP00/PAE99-080TRDE
P22953

Claims:

1. Method for the authentication of data communicated from a originator to a destination,
wherein a keyed hashing technique is used, according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function, and the data are transmitted together with the digest of the hash function from the originator to the destination,
characterized in that
the data comprises temporal validity information representing the temporal validity of the data.

2. Method according to claim 1,
characterized in that
the temporal validity information can be defined by the originator.

3. Method according to anyone of the preceding claims,
characterized in that
the data comprises random data which are unique for a time span defined by the temporal validity information.

4. Method according to anyone of the preceding claims,
characterized in that
the data is a login key for a communication setup and/or a message.

5. Method for the authenticated transmission of messages,

comprising the following communication setup steps:

- generating a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key,
- transmitting the login key from an originator to a destination, and
- verifying the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest on the destination side.

6. Method according to claim 5,

furthermore comprising the following acknowledgment steps:

in case the verification of the authenticity and the temporal validity of the login key is positive,

- generating an acknowledgment key by a keyed-hashing method on the basis of second random data and the private key,
- transmitting the acknowledgment key from the destination to the originator, and
- verifying the acknowledgment key by the originator.

7. Method according to claim 6,

characterized in that

the acknowledgment key furthermore comprises a time stamp and when verifying the acknowledgment key it is checked on the basis of the time stamp and the temporal validity information whether the acknowledgment key is still valid..

8. Method according to claim 6 or 7,

furthermore comprising the following message transmission steps:

in case the verification of the acknowledgment key is positive,

- extracting the second random data from the acknowledgment key,
- generating a message by a keyed-hashing method on the basis of the second random data, message data and the private key,
- transmitting the message from the originator to the destination, and,
- verifying the message by the destination.

9. Method according to claim 8,

characterized in that

the message furthermore comprises a time stamp and when verifying the message it is checked on the basis of the time stamp and the temporal validity information whether the message is still valid.

10. Software program product,

characterized in that

it implements, when loaded into a computing device of a distributed system, a method according to anyone of the preceding claims.

11. Distributed system for communicating authenticated data from a originator to a destination,

designed for a keyed hashing technique according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function, and the data are transmitted together with the digest of the hash function from the originator to the destination,

characterized in that

the data comprises temporal validity information representing the temporal validity of the data.

12. Distributed system according to claim 11,

characterized in that

the originator is designed to define the temporal validity information.

13. Distributed system according to claim 11 or 12,

characterized in that

the data comprises random data which are unique for a time span defined by the temporal validity information.

14. Distributed system according to anyone of claims 11 to 13,

characterized in that

the data is a login key for a communication setup and/or a message.

15. Distributes system for the authenticated transmission of messages, comprising:
- an originator designed to generate a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key,
- a network for transmitting the login key from the originator to a destination,
wherein the destination is designed to verify the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest.

16. Distributed system according to claim 15 ,
wherein the destination is designed to generate an acknowledgment key by a keyed-hashing method on the basis of second random data and the private key and to transmit the acknowledgment key to the originator in case the verification of the authenticity and the temporal validity of the login key is positive, and
the originator is designed to verify the acknowledgment key.

17. Distributes system according to claim 16,
characterized in that
the acknowledgment key furthermore comprises a time stamp and when verifying the acknowledgment key the originator checks on the basis of the time stamp and the temporal validity information whether the acknowledgment key is still valid..

18. Distributed system according to claim 16 or 17,
characterized in that
the originator is designed to extract the second random data from the acknowledgment key in case the verification of the acknowledgment key is positive, generate a message by a keyed-hashing method on the basis of the second random data, message data and the private key, and transmit the message to the destination, and the destination is designed to verify the message.

19. Distributed system according to claim 18,
characterized in that

the message furthermore comprises a time stamp and when verifying the message, the destination checks on the basis of the time stamp and the temporal validity information whether the message is still valid.